Social Engineering & Awareness in Turkey

Bariskan, M. A [1,2] , Aydin, M. A.[1]
[1] Computer Engineering Dept., Faculty of Engineering, Istanbul University, Istanbul, Turkey
[2] Computer Engineering Dept., Faculty of Engineering & Architecture, Istanbul Gelisim University, İstanbul, Turkey

E-mail: mabariskan@gelisim.edu.tr

ABSTRACT - Rapid changes in technology threaten the reliability of the country's systems while trying to catch the world in terms of technology. With the development of the Internet of Things in recent years, security has become a serious situation. The biggest DDOS work that has been done so far is not with computers, but small smart devices like ipcam, tv, washing machine with internet connection. Information such as the user name and password used in the control of these devices can easily be captured by the methods of collecting information from Social Engineering. Especially when we think that according to wearesocial research 63% of the total population and 80% of 13+ age population of Turkey is a social media user as of the end of 2018 and 29% of the internet users use social media for work so the information that people share can be an appetite for attackers. In this research, we examined the usage habits of the people of Turkey and look at what measures are necessary to protect Turkey.As we take account of this dark results we learned that we must take more measurements to make Turkey safe

Keywords: Cyber Security, Turkey, Cyber Fraud, Social Engineering.

1. INTRODUCTION

With the rise of intelligent technologies in today's world, cyber security is becoming increasingly important, especially with the emergence of ”Internet of Things“ Up to now, the world's largest DDOS attack has not been done on computers, but on other small processor devices (smart television, IP cameras, etc.). This increases the importance of communication and behavior of people with these devices.

The international data company Digital Guardian defined social engineering as follows. Social Engineering is a non-technical strategy that uses standard security practices to deceive people. The success of social engineering techniques depends on the ability of attackers to direct victims to specific activities or to provide confidential information. Today, social engineering is recognized as one of the biggest security threats faced by organizations. Social engineering differs from traditional cyber attacks in that social engineering does not require non-technical and reconciliation or exploitation of software or systems. When successful, many social engineering attacks allow attackers to provide legitimate, authoritative access to confidential information.

Considering that the term cyber world now includes telephones, phone fraud also falls within the sphere of cyber security. Phone scams. Most of the time, information is obtained using social media. Location sharing applications such as foursquare and Instagram have become the centers where perverts use to select targets.

According to the 2019 January report of the international social media research company We are Social (Digital In 2019: Global Overview, 2019), 57% of the average population in the world is up to 72% in Turkey pass time on internet. This means a 9,1% increase(In Turkey) in 2018 compared to the previous year. According to the same report, about 7:15 hours of day we spend on the internet and we spend 2:46 hours of these 7:15 hours on social media, with these data the importance of the information we share when we are on internet arises.

However, in these times when we are in the middle of the informatics era, the world is now being managed and shaped over the internet. The Facebook influence in the Arab Spring (Huang C., 2011) has spread from one country to another and has ultimately changed the political structure of northern Africa. In addition, Facebook's service “I'm good” offered to people in natural disasters, at the terrorist attacks by providing the news from each other by ensuring that the main goal of terrorism is helping to create a chaos.

In addition to these studies, it is seen that intelligence organizations have begun to realize the social movements' development of social movements (social media tools with social engineering methods like emotion analysis, orientations etc.) (Aliprandi C. De Luca A.E. Pietro G.D. 2014).

2. SOCIAL ENGINEERING

According to the report of the UK National System Protection Center, Social Engineering can be defined in many ways within the psychological and security boundaries. It is mainly defined as using the people to break the security of an institution. Kevin Mitnick, the FBI's most-wanted computer hacker, is described as seizing critical information by persuading, manipulating, using people's naivety. However, in the simplest terms, it can be defined as gaining people's confidence and making them do what they do not want to do.

2.1. Social Engineering Phases.

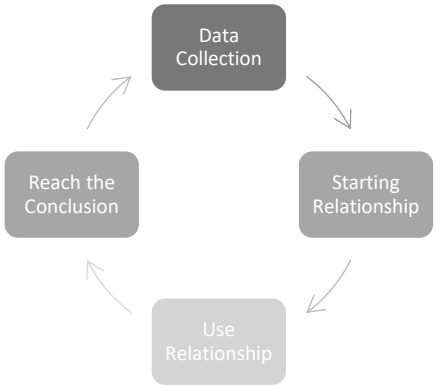

Figure 1 Social Engineering Circle

Unfortunately, Data collection phases are provided very easily, becouse of unconscious social media uses, web sites, workplace web pages, etc.. In the second phase, the attacker develops a relationship with the victim by using the information he / she acquires. In the third phase, the information of the aggressive person who gained the trust of the victim, credit card information, login passwords and so on. Finally, the attacker accomplishes his goal, which may be one of the previous steps(Fig.1).

2.2. Types of Social Engineering Methods

Social engineering attacks are usually divided into two different categories. These are Physical location (computer based) attacks and Psychological-Emotional attacks.

2.2.1. Attack Methods Through Physical Locations

Computer-based attacks are usually attacks that are intended to capture victims using technology.

Types of attacks in the workplace are usually the most difficult species. Here the attacker needs to replace an employee individually. These low-level employees are often in the background to eavesdrop the information of employees and companies.

Phone attacks are the most prominent attacks in Turkey. They are customer service, municipal staff, municipal police, public prosecutor, military, police, paramedics and so on. In this way, people who know their way to help their victims by threatening them with the help of threats and help.

The online method evolves over the victim's e-mail, through instant messaging platforms or through messages sent over social media to request information about the person. Such attacks are often referred to as penetration attacks.

2.2.2. Psychological Methods

Popular and easy Social Engineering still remains on human basis. Emphasis and interpersonal relations are emphasized by using certain techniques such as declining, intimidation, disdain, authority and lubrication (Hadnagy C. 2013). It is based on the use of one-to-one communication between the attacker and the victim. For the most part, this methodology is based on the realization of a background study of information acquisition in the targeted organization. Some of the techniques used to gather this information are: shoulder-to-ear listening and ear relief. Once the basic knowledge acquisition is guaranteed, it is used to manipulate the target to obtain additional information, as described in the next section.

Authority: It is a source of effective information gathering from an innocent target, in particular a newly hired employee or a low-level staff member. The most common method is to use an attacker's security partition, IT department, manager, or other high-level authority to obtain information about the new password through password detection or threat or intimidation. For example, the attacker may threaten to report to his / her supervisor due to a lack of staff, or the target staff may threaten to think that they are late to submit important data or information to the general manager of the organization. Such actions allow the sighting of feared or threatened staff to request information. This method is highly effective in hierarchical organization.

Natural Feeling to Help: People tend to help people in need. Unfortunately, this feature is known to social engineers who benefit from this human nature. For example, a social engineer can imitate a delivery man who carries many boxes at a workplace and physically access a target building by an employee deciding to keep the door open. In another case, an attacker can mimic a desperate employee who calls the IT help desk to access the corporate network from home and cause the attacker to get sensitive information about corporate networks.

Likes and Similarities: By speaking comfortably, an attacker can have an idea on a target that aims to develop links. For example, sharing similar activities and hobbies, supporting the same sports team, or claiming the origin or country. There is a natural tendency for people to be associated with people with similar interests or origins. In this process, an attacker can establish a relationship that makes it easier for them to obtain sensitive information while relying on them.

Commitment and Consistency: In this method, which usually works on the victims who want to prove their new job, the assailant may ask the victim to enter something new in the system. And in the meantime, you can capture your

login information. In this case, the victim may become a criminal.

Reciprocity: The norm in social interactions states that if someone gives us something, it will be respectful only if goodness returns to goodness. This method is called reverse social engineering. The technique causes the attacker to create a situation that faces a problem with the victim, and that the target in question seeks help from the attacker who is solving the situation. In return, the victim feels compelled to help the attacker.

Initiatives by Fake Legal Officers: Psychological attacks in Turkey is the most experienced type of attack. These people, who often present themselves as police officers, MIT agents, prosecutors or soldiers, are saying that the person or his family is involved in a legal job. They can do what they want by saying that people should be in corporation with them.

3. CYBER SECURITY AWARENESS IN TURKEY

As cyber security becomes a topic that increases its effectiveness on the world, the awareness of the users about it becomes more important.

ISA (International Security Agency) tends to focus on definitions in two directions. First, employees understand their security information security behaviors, which are usually summarized in their information security policies, rules and guidelines (Bulgurcu et al., 2010; Kruger and Kearney, 2006). For example, Kruger and Kearney (2006), lad we need to know how each member of staff understands the importance of information security, the level of information security appropriate for the organization, and the individual security responsibility. Örneğin (p 289). The second issue focuses on how little employees are working and generally to comply with the best practices outlined in information security policies, rules and guidelines (Kruger H. and Kearney, W. 2006; Siponen, M.T. 2000). Therefore, the ISA should consider the extent to which an organization's employees understand the importance and consequences of information security and the extent to which the organization acts in accordance with information security policies and procedures. This definition supports the Information-Attitude-Behavior (BTD) * model, Human Aspects of Information Security Questionnaire (Human Factor in HAIS-Q-Cyber Security Queries). Based on the BTD model, the attitudes are improved and the information security behavior is improved as the employee's knowledge of the secure information security behaviors at the workplace increases (Parsons et al., 2014a).

The questionnaire used in this study was prepared to search for entry-level cyber security information in Turkey. As can be seen in the Findings section, the situation proves that most people are ignored as simple security behaviors.

Social engineering, which is the subject of this article, has been focused on people and 19 questions about this subject has been prepared by taking into consideration the previous researches. The questions in this questionnaire tried to find out the openness to the social engineering attacks of the participants during the use of computers.

Although the majority of the respondents were university students (18-23 age group), people from all ages and education levels participated. Age distribution of the respondents is as follows. It is thought that the age of the respondents at the age of 13 is the same as the other answers in the questionnaire. The age distribution is shown in figure 2.

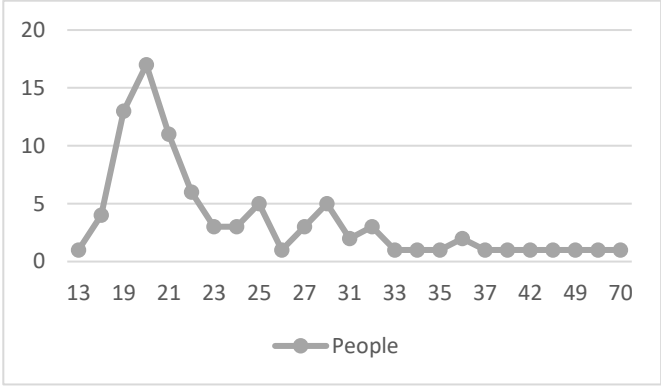

Figure 2 Age Distiribition of People Who Answered This Questionair

The demographic distribution of the educational status of the respondents is as follows. According to this, a rate of 95% is higher and higher. 2% of high school graduates and 1% of primary school graduates. The remaining 2% was completed or completed a 2-year college education. The gender distribution was 55% male and 45% female as shown in Figure 3 and 4

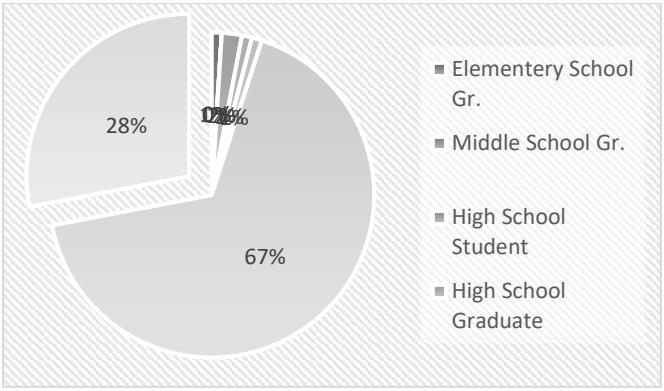

Figure 3 Educational Distibution

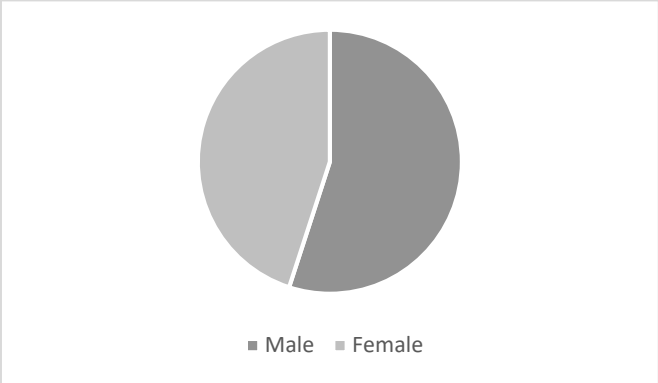

Figure 4 Gender Distribution

The regression of Facebook shares according to educational status and knowledge level is shown in Figure 5. Accordingly, the increase in the level of education and the level of knowledge has led to more attention on Facebook shares.

However, Figure 6 shows the regression of the control ratio in the e-mail attachments according to the level of education and knowledge level. Accordingly, it was seen that the education level and the rate of information directly affected the rate of e-mail control.

When two graphs are compared, it is understood that participants are more careful in controlling e-mails than they share in Facebook.

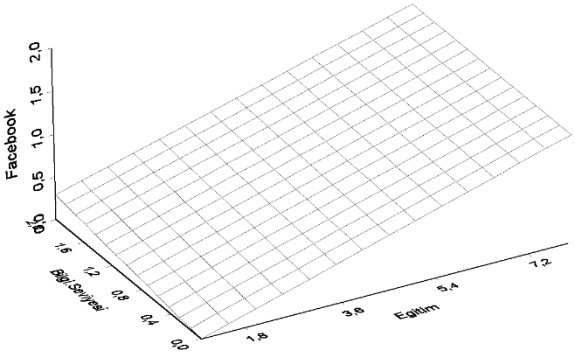

Figure 5 Regression of Facebook Shares According to Level of Education and Level of Knowledge

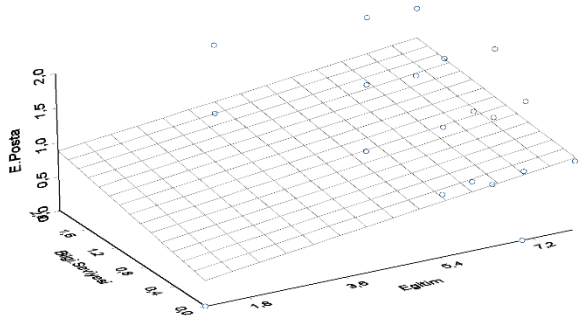

Figure 6 Regression of the Control Ratio in E-Mail Attachments According to Level of Education and Level of Knowledge

4 DISCUSSION AND CONCLUSION

When the above information is examined, it is understood that most of the participants have input level information about cyber security but unfortunately they have very little news about social engineering attacks. In particular, they do not know how dangerous the social media sharing can be (Buchanan T, Paine C, Joinson AN, Reips UD. 2007).

Facebook and Instagram over the following abuses, scams carried out on Facebook, phone scams are collected by gathering information about people. An example of this is the, Oktay Doğan 201 child abuser, who was revealed in March by a conscious family (Bitki H.İ. Milliyet, 2017). It is an indisputable fact that individuals should be educated against such attacks.

The forms of these trainings should vary according to the cultures and should be prepared and implemented at the regional level.

At the country level, what should be done is to increase the security measures and to understand the individuals' sharing habits and re-prepare the security questions and inform them about the e-mail attacks and the deliberate attacks.

References

Huang C. 2011, Facebook and Twitter key to Arab Spring uprisings: report ,The National

Digital In 2019: Global Overview, 2019

Aliprandi C. De Luca A.E. Pietro G.D. 2014, CAPER: Crawling and analysing Facebook for intelligence purposes , Advances in Social Networks Analysis and Mining (ASONAM), 2014 IEEE/ACM International Conference on 17-20 Aug. 2014

Hadnagy C. 2013, Sosyal Mühendislik: İnsanı Kandırma Sanatı,Paloma,İstanbul

Bulgurcu B, Cavusoglu H, Benbasat I. 2010 Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quart;34(3): 523–48.

Kruger H, Kearney W. 2006 A prototype for assessing information security awareness. Comput Secur;25(4):289–96.

Siponen M.T.2000 A conceptual foundation for organizational information security awareness, Information Management & Computer Security

Parsons K, McCormac A, Butavicius M, Pattinson M, Jerram C. 2014 Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). Computer Security 2014a;42:165–76.

Bitki H.İ.Milliyet,2017, Facebook'taki sapığa dikkat! http://www.milliyet.com.tr/ facebook-taki-sapiga-dikkat-gundem-2212152/

Buchanan T, Paine C, Joinson AN, Reips UD. 2007 *Development of measures of online privacy concern and protection for use on the Internet*. J Am Soc Inf Sci Technol;58(2):157–65.